INFORMATION AND COMPUTATION 91, 172–176 (1991)

Computing the Order of Centralizers in Linear Groups

LAJOS RÓNYAI*

Hugarian Academy of Sciences, Budapest H-1132, Hungary, and
University of Chicago, Chicago, Illinois 60637

In this note we give a polynomial time algorithm to compute the order of the centralizer of a given subgroup of a full linear group over a finite field. The method is deterministic if the characteristic of the ground field is small and Las Vegas in the general case. As an application we show that the verification of the center of a linear group over a finite field belongs to the complexity class AM. This settles a question of L. Babai.

1. INTRODUCTION

First we introduce some notation. F_q denotes the finite field with $|F_q| = q$ and $GL(n, F_q)$ stands for the group of all nonsingular n by n matrices over F_q. The centralizer $C(G)$ of a subgroup $G \leqslant GL(n, F_q)$ is defined as

$$C(G) = \{A \in GL(n, F_q);\ BA = AB, \text{ for all } B \in G\}.$$

Clearly $C(G)$ is a subgroup of $GL(n, F_q)$. The subgroup $Z(G) = C(G) \cap G$ is the center of G. The order of a finite group G is the number of elements of G. We consider the following algorithmic problem.

CENTRALIZER (k, n, q).

INPUT: A collection of matrices $A_1, A_2, ..., A_k \in GL(n, F_q)$.
OUTPUT: The order of $C(G)$ where G is the group generated by the matrices A_i.

A matrix is given as an array of n^2 elements of F_q. The field F_q is specified by the minimal polynomial $f(x) \in F_p[x]$ of a generating element γ of the extension F_q/F_p, where F_p is the prime field of F_q. In particular, f is irreducible over F_p and if $q = p^s$ then $\deg(f) = s$. An element $\alpha \in F_q$ can now be represented in the form $\alpha = a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{s-1}\gamma^{s-1}$, where $a_i \in F_p$. The result of this paper is the following.

* Research partially supported by Hungarian National Foundation for Scientific Research Grant 1812.

0890-5401/91 $3.00

THEOREM. *Centralizer* (n, k, q) *can be solved in Las Vegas time polynomial in* $n, k,$ *and* $\log q$. *Also it can be solved by a deterministic algorithm running in time polynomial in* n, k, p, *and* s.

Note that the randomized time bound is polynomial in the input size.

The *center problem* for linear groups is the recognition problem of the "language" $\{(q, n, G_1, G_2);\ G_1, G_2 \leqslant GL(n, q),\ G_2 = Z(G_1)\}$. Here G_1, G_2 are given by generating sets and the generators are elements of $GL(n, F_q)$.

COROLLARY. *The center problem for linear groups belongs to the complexity class AM.*

For a background on Arthur–Merlin protocols the reader is referred to Babai (1985, 1989).

Proof. Using the randomized algorithm for Centralizer ( ) Arthur computes first the order o of $G = C(G_1)$ and verifies (in deterministic polynomial time) that G_2 centralizes G_1. Next Merlin guesses a short (i.e., $m \leqslant n^2 \log q$) system of generators $B_1, ..., B_m$ of G and the orders o_1, o_2, o_3 of the groups G_1, G_2, and $G_3 = G_1 G$, respectively. Finally using the AM protocols from Babai (1989) they verify the following statements:

1. The matrices B_j generate G.
2. The order of G_i is o_i for $i = 1, 2, 3$.
3. $G_2 \leqslant G_1$. Upon completion Arthur accepts if and only if $o_3/o = o_1/o_2$.

The significance of statement 1 is that the protocol for statement 2 works for groups given by generators. Statement 1 is verified by a protocol for the order of the group H generated by the matrices B_i. Arthur can check himself if $H \leqslant G$ in the straightforward way. Arthur accepts that $H = G$ iff $|H| = |G|$ and $H \leqslant G$.

Statement 3 certifies that $G_2 \leqslant Z(G_1)$ and therefore it suffices to verify the order of $Z(G_1)$. The isomorphism $G_1 C(G_1)/C(G_1) \cong G_1/Z(G_1)$ implies that the order of $Z(G_1)$ is o_2 iff $o_3/o = o_1/o_2$. ∎

2. PROOF OF THE THEOREM

Here we describe the method to solve the problem Centralizer ( ). We shall work with associative algebras having an identity element 1. For such an algebra $\mathscr{A}$ let $U(\mathscr{A})$ denote the group of invertible elements (units) of $\mathscr{A}$.

First we compute a basis over F_q of the centralizer algebra

$$\mathscr{A} = \{A \in M_n(F_q);\ AA_i = A_iA \text{ for } 1 \leqslant i \leqslant k\}$$

of the group G generated by the matrices A_i. Clearly we have

$$C(G) = \mathscr{A} \cap GL(n, F_q) = U(\mathscr{A}).$$

Note that a basis of $\mathscr{A}$ is obtained by solving a system of linear equations over F_q derived from the definition of $\mathscr{A}$ above. Consequently the cost of computing $\mathscr{A}$ is $(n+k+\log q)^{O(1)}$. By Wedderburn's theory of finite dimensional associative algebras (cf. Herstein, 1968; Pierce, 1982) $\mathscr{A}$ has a unique maximal nilpotent ideal

$$\mathrm{Rad}(\mathscr{A}) = \{A \in \mathscr{A};\ 1 + AB \in U(\mathscr{A}) \text{ for every } B \in \mathscr{A}\}, \tag{1}$$

the radical of $\mathscr{A}$.

The factor algebra $\mathscr{B} = \mathscr{A}/\mathrm{Rad}(\mathscr{A})$ can be expressed as

$$\mathscr{B} = \mathscr{B}_1 \oplus \mathscr{B}_2 \oplus \cdots \oplus \mathscr{B}_m, \tag{2}$$

where the $\mathscr{B}_i$ are simple algebras over F_q and they are the (uniquely determined) minimal ideals of $\mathscr{B}$. The algebras $\mathscr{B}_i$ are isomorphic to full matrix algebras. More precisely there exist integers n_i and finite extension fields $F^{(i)} \geqslant F_q$ such that

$$\mathscr{B}_i \cong M_{n_i}(F^{(i)}). \tag{3}$$

These structural components of $\mathscr{A}$ can be computed efficiently. A basis of $\mathrm{Rad}(\mathscr{A})$ can be found in deterministic polynomial time (Friedl and Rónyai, 1985, Sect. 5; Rónyai, 1990, Section 2). The ideals $\mathscr{B}_i$, the fields $F^{(i)}$ and the numbers n_i are obtained in Las Vegas time $(n+k+\log q)^{O(1)}$ or in deterministic time $(n+k+p+s)^{O(1)}$ (Friedl and Rónyai, 1985, Sect. 7.3; Rónyai, 1990, Sect. 3).

The natural map $\mathscr{A} \to \mathscr{B}$ induces an epimorphism of groups $\phi\colon U(\mathscr{A}) \to U(\mathscr{B})$. Also from (2) we have

$$U(\mathscr{B}) = U(\mathscr{B}_1) \times U(\mathscr{B}_2) \times \cdots \times U(\mathscr{B}_m). \tag{4}$$

We infer that it suffices to find the orders for the groups $U(\mathscr{B}_i) = GL(n_i, F^{(i)})$ and $H = \ker \phi$, respectively. Now if r_i denotes the order of the field $F^{(i)}$ then for the order l_i of $U(\mathscr{B}_i)$ we have the well-known (and easily computable) formula

$$l_i = (r_i^{n_i} - 1)(r_i^{n_i} - r_i) \cdots (r_i^{n_i} - r_i^{n_i - 1}).$$

From (1) we infer that

$$H = \{1 + A;\ A \in \mathrm{Rad}(\mathscr{A})\}$$

and consequently $|H| = |\mathrm{Rad}(\mathscr{A})|$. Putting these together we obtain the efficiently computable formula for the order of $C(G)$:

$$|C(G)| = l_1 l_2 \cdots l_m |\mathrm{Rad}(\mathscr{A})|.$$

This completes the proof. ∎

3. A Concluding Remark

It would be interesting to find efficiently generators for $C(G)$. This problem is equivalent to finding generators for the groups $U(\mathscr{B}_i)$ and H. We can construct generators for H in deterministic polynomial time as follows. Let d be the smallest positive integer such that for the ideal $\mathscr{I} = \mathrm{Rad}(\mathscr{A})$ we have $\mathscr{I}^d = (0)$. Note that $\mathscr{A} \leqslant M_n(F_q)$ implies that $d \leqslant n$. For $j = 1, \ldots, d-1$ let X_j be a subset of $\mathscr{I}^j$ such that the images under the natural map of the elements of X_j form a basis over F_q of the linear space $\mathscr{I}^j/\mathscr{I}^{j+1}$. Now we set $X = X_1 \cup X_2 \cup \cdots \cup X_{d-1}$. It is easily seen that the set

$$S = \{1 + A;\ A \in X\}$$

is a generating system of H.

We are, however, unable to construct generators for the $U(\mathscr{B}_i)$ in Las Vegas polynomial time. Using the methods of Rónyai (1987, Sect. 6.1; 1990, Sect. 5.1), the isomorphisms in Eq. (3) can be constructed in Las Vegas time $(n + k + \log q)^{O(1)}$ or in deterministic time $(n + k + p + s)^{O(1)}$. This means that it would suffice to find generators for the groups $GL(m, F)$, where F is a finite field. We can construct generators for the large normal subgroup

$$SL(m, F) = \{A \in GL(m, F), \det(A) = 1\}.$$

It is known (cf. Suzuki, 1982, Theorem 9.2) that $SL(m, F)$ is generated by the two subgroups

$$U(m, F) = \{I + A;\ A_{ij} = 0 \text{ if } i \geqslant j\}$$

and

$$L(m, F) = \{I + A;\ A_{ij} = 0 \text{ if } i \leqslant j\},$$

where I is the identity matrix. But if $\mathscr{A}$ denotes the algebra of matrices

$$\mathscr{A} = \{\lambda I + A;\ \lambda \in F \text{ and } A_{ij} = 0 \text{ if } i \geqslant j\}$$

then we have

$$U(m, F) = \{I + A;\ A \in \mathrm{Rad}(\mathscr{A})\}$$

and therefore our previous construction gives generators for $U(m, F)$. The group $L(m, F)$ can be treated analogously. We can therefore obtain generators for $SL(m, F)$ in deterministic time $(m + \log |F|)^{O(1)}$. We could easily augment this to obtain a generating set for $GL(m, F)$ if we had generators for the multiplicative group F^*. Unfortunately it is not known if a generating system of the multiplicative group F^* can be obtained in Las Vegas time polynomial in $\log|F|$. Note also, that this is a special case of our original problem because $GL(1, F) = F^*$. These imply that the problems of finding generators for $GL(m, F)$ and for F^* are equivalent up to deterministic polynomial time reductions.

RECEIVED June 19, 1989; FINAL MANUSCRIPT RECEIVED August 30, 1989

REFERENCES

BABAI, L. (1985), Trading group theory for randomness, *in* "Proceedings, 17th ACM Symp. on Theory of Computing," pp. 421–429.

BABAI, L. (1989), Interactive proofs in finite groups, *SIAM J. Discrete Math.*, to appear.

FRIEDL, K., AND RÓNYAI, L. (1985), Polynomial time solutions of some problems in computational algebra, *in* "Proceedings, 17th ACM Symp. on Theory of Computing," pp. 153–162.

HERSTEIN, I. N. (1968), "Noncommutative Rings," Math. Assoc. of Amer., Washington, DC.

PIERCE, R. S. (1982), "Associative Algebras," Graduate Texts in Mathematics, Vol. 88, Springer-Verlag, New York/Berlin.

RÓNYAI, L. (1987), Simple algebras are difficult, *in* "Proceedings, 19th ACM Symp. on Theory of Computing," pp. 398–408.

RÓNYAI, L. (1990), Computing the structure of finite algebras, *J. Symbolic Comput.* **9**, 355–373.

SUZUKI, M. (1982), "Group Theory I," Grundlehren Math. Wissen., Vol. 247, Springer-Verlag, New York/Berlin.